

Recipe 12 – Configuration Guide for Setting up HP Select Access 5.2 as a CS

Table of Contents:

1	Setup	1
1.1	Terms and Introduction.....	1
1.2	Using the Setup Tool	2
2	Policy Builder	5
2.1	Using Policy Matrix to modify SAML component configuration	5
2.2	Adding an AA.....	8
2.3	Adding SAML Assertion Attribute	10

Version 2.0.0

1 Setup

1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and HP Select Access 5.2 as a Credential Service (CS). Remember that the HP Select Access setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the main screen shown in Figure 12-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

1.2 Using the Setup Tool

Use the setup tool to configure a SAML server. Accessing the set up program is the same whether you are setting up a CS or an AA. After the initial setup, do not attempt to use the setup tool again. Instead, use SAML partner properties to access properties

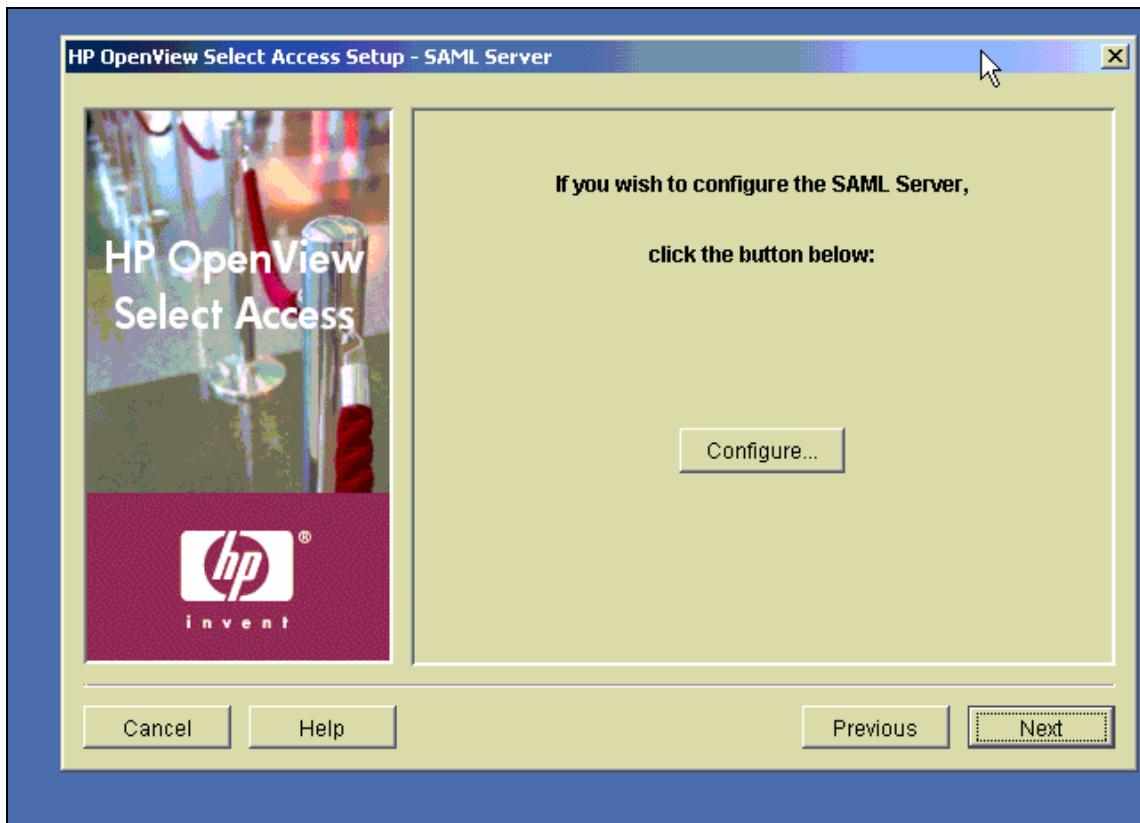


Figure 12-1: Start Setup Tool



Figure 12-2: Select Access Setup



Figure 12-3: Define SAML Server ID

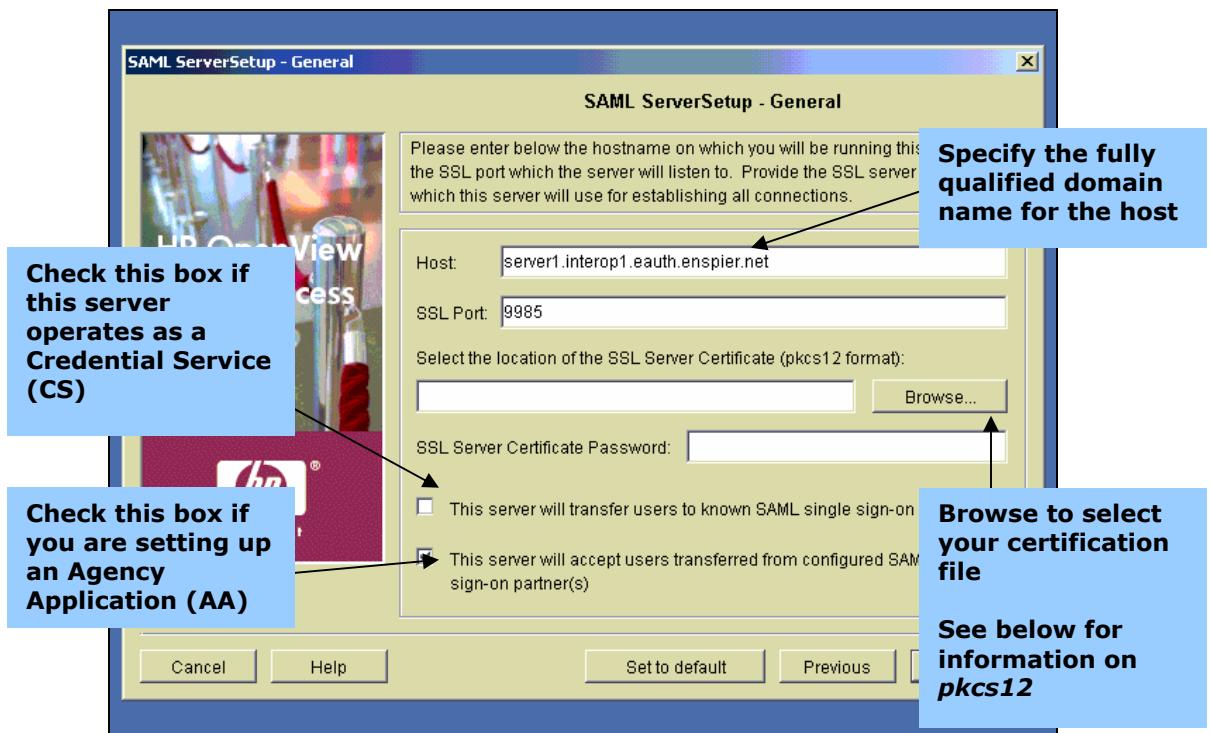


Figure 12-4: General Server Setup

PKCS12 files combine private and public key certificates. The PKCS12 file is protected by a password, which you will provide when you create your PKCS12 file.

2 Policy Builder

2.1 Using Policy Matrix to modify SAML component configuration

From the Policy Administration screen click on *Tools*, and then select *Component Configuration*.

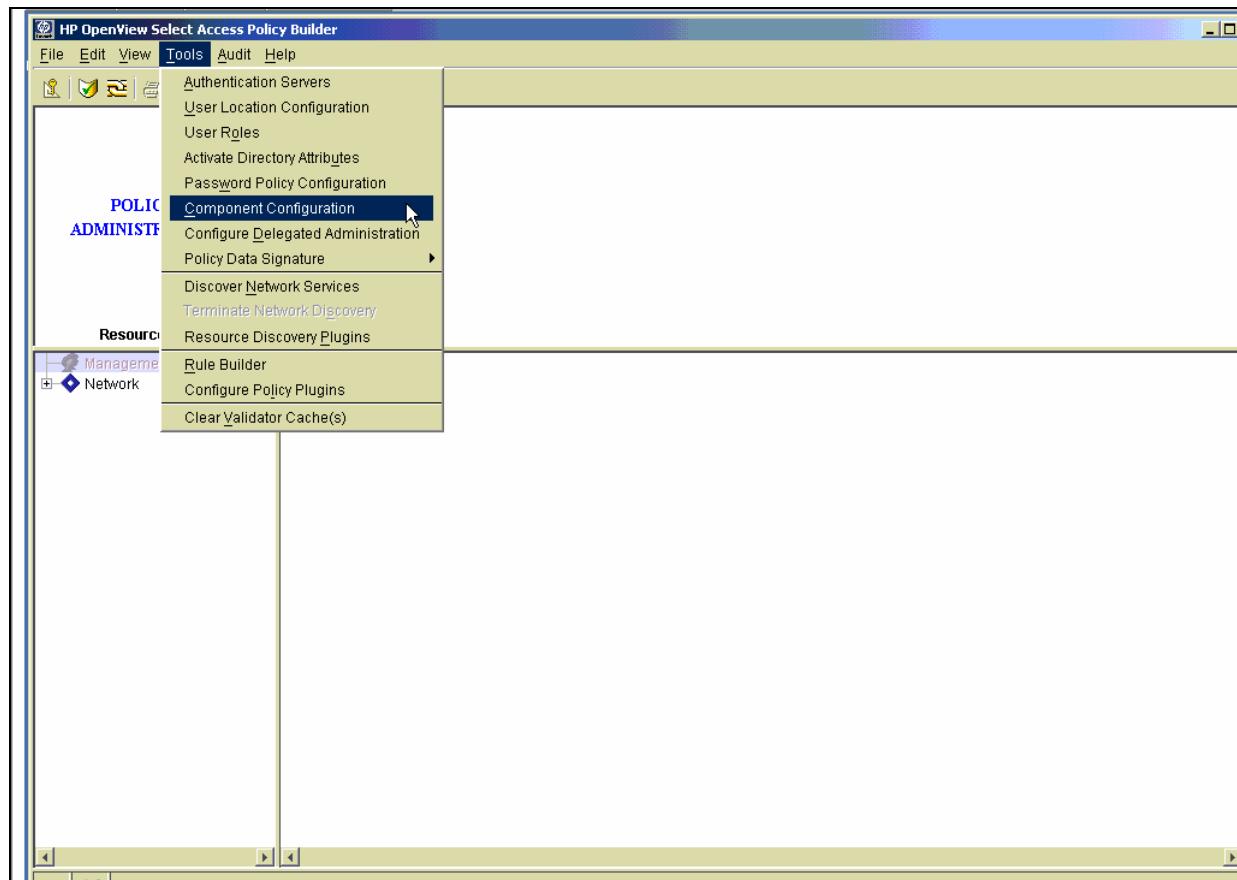


Figure 12-5: Working with Policy Builder

A component configuration window will open, as shown in Figure 12-6 below. To view assertion properties, right click on a SAML server file, choose *Properties*

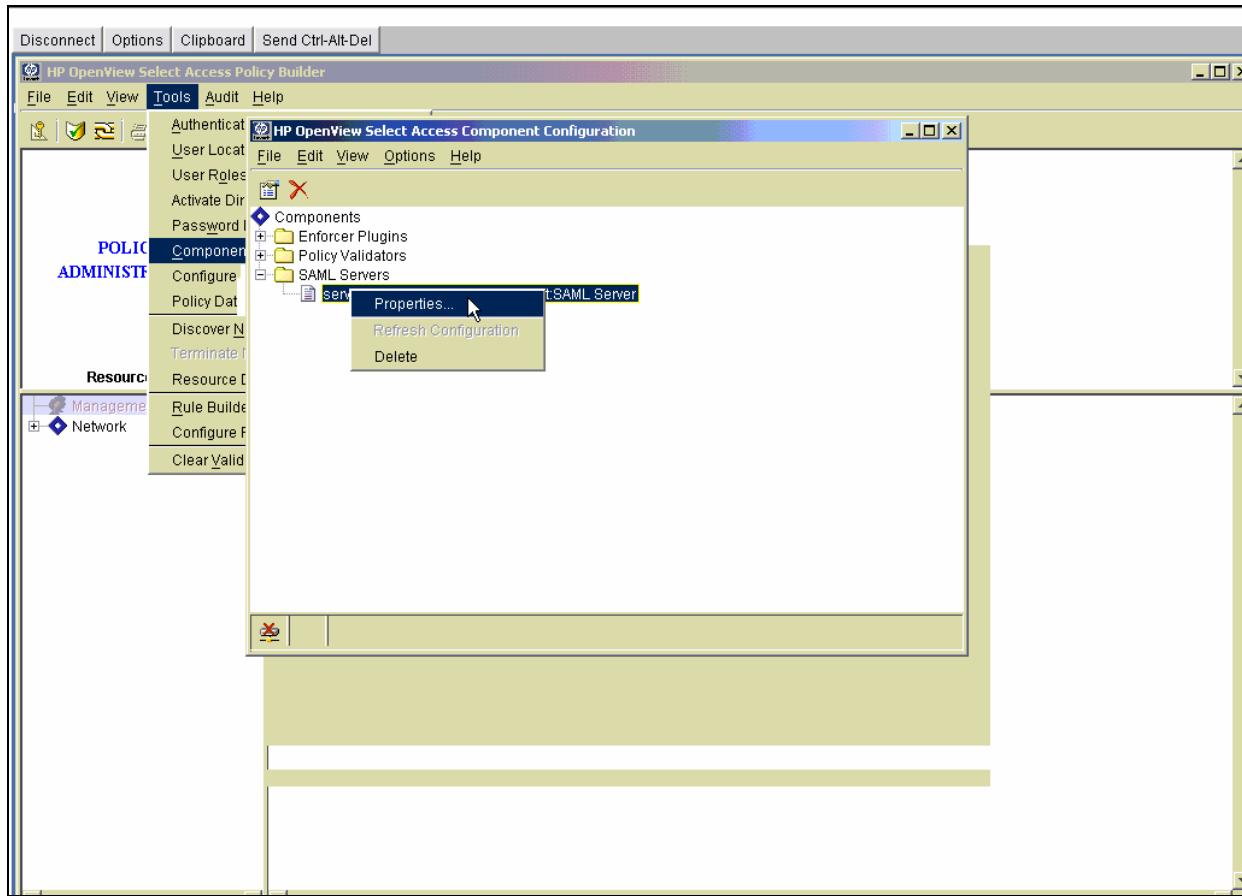


Figure 12-6: Navigating to Component Configuration

A window for assertion properties, as shown in Figure 12-7, will open.

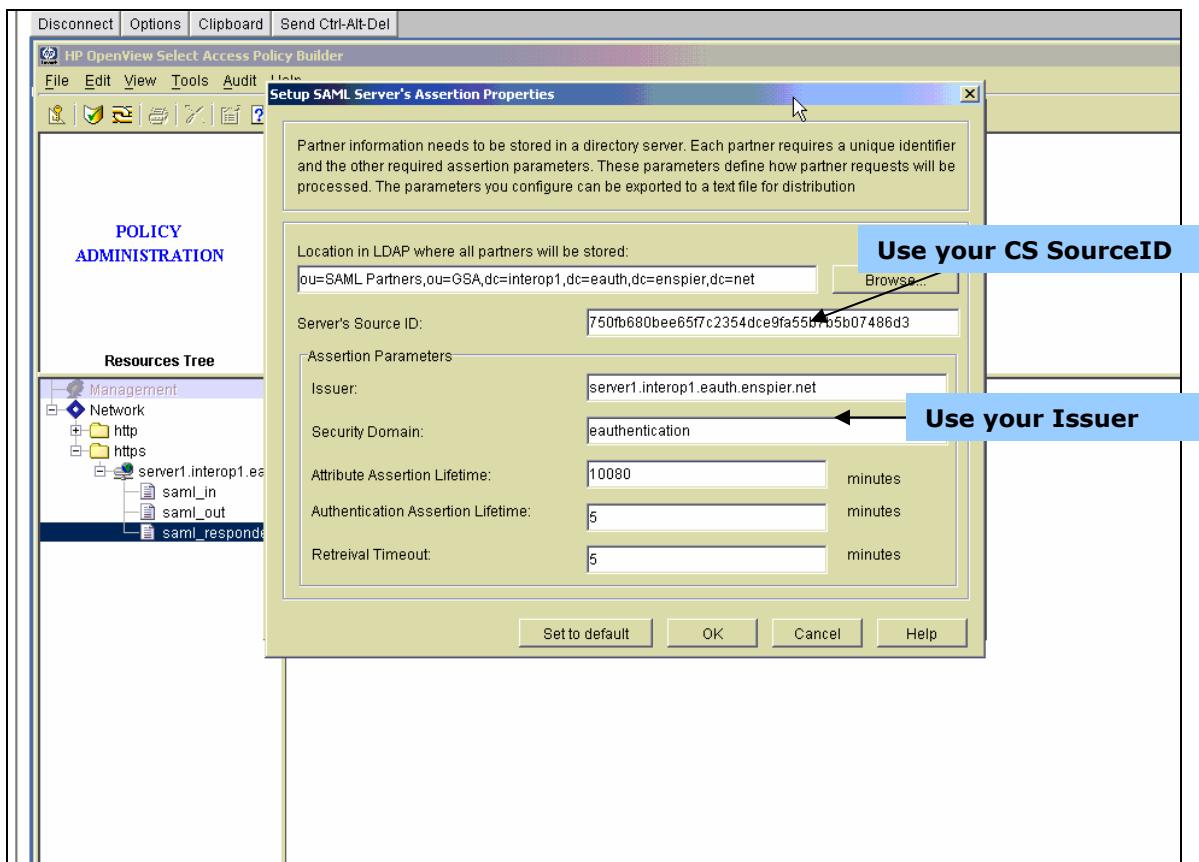


Figure 12-7: Configure AA Assertion Properties

2.2 Adding an AA

If you click on Configure, the *Setup SAML Server's Assertion Properties* window will display, as shown in Figure 12-8. This information is also found in the setup tool, but it is best to configure through the steps defined in section 2.5.

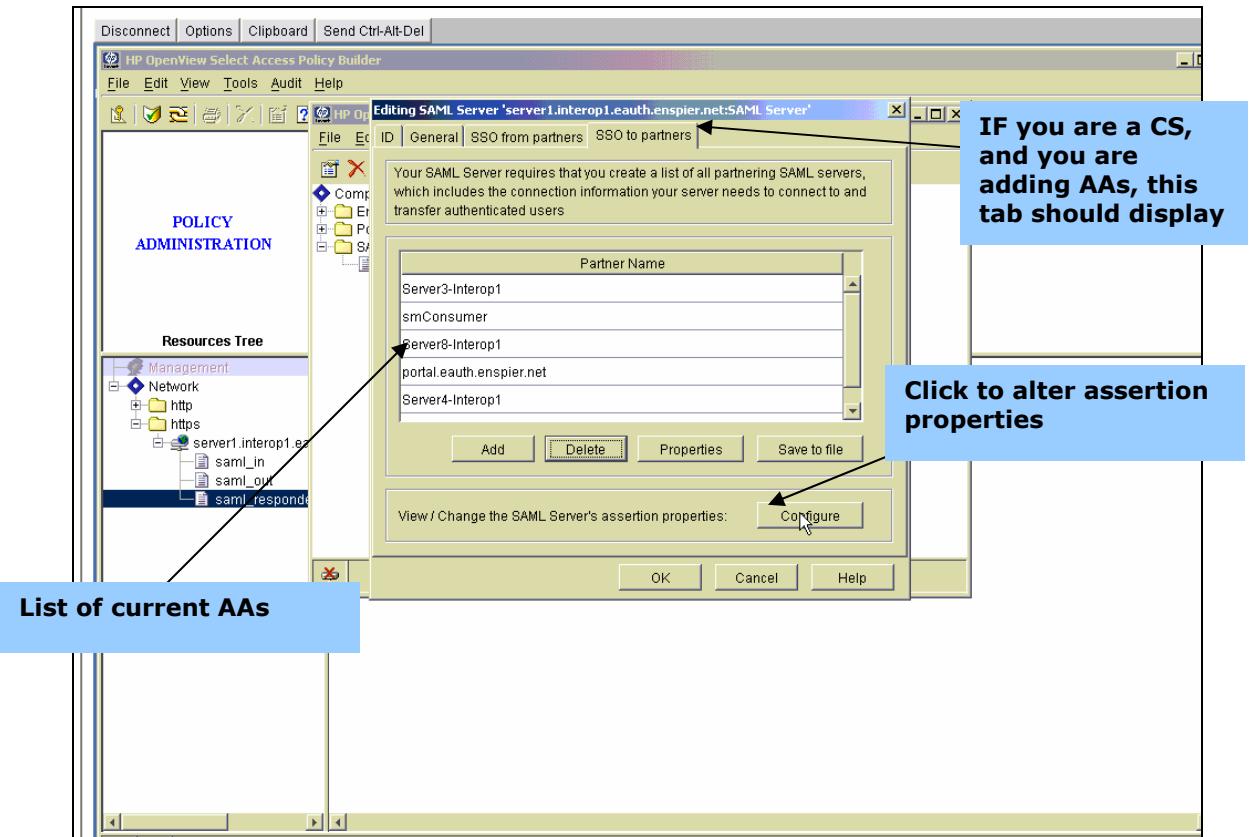


Figure 12-8: Starting point for modifying and adding new AAs

After you click on the *Add* button, see figure 12-9, the *Setup SAML destination partner* window will display. Enter your *Name*, *URL Alias*, etc., and then click on *OK* to finish and save settings.

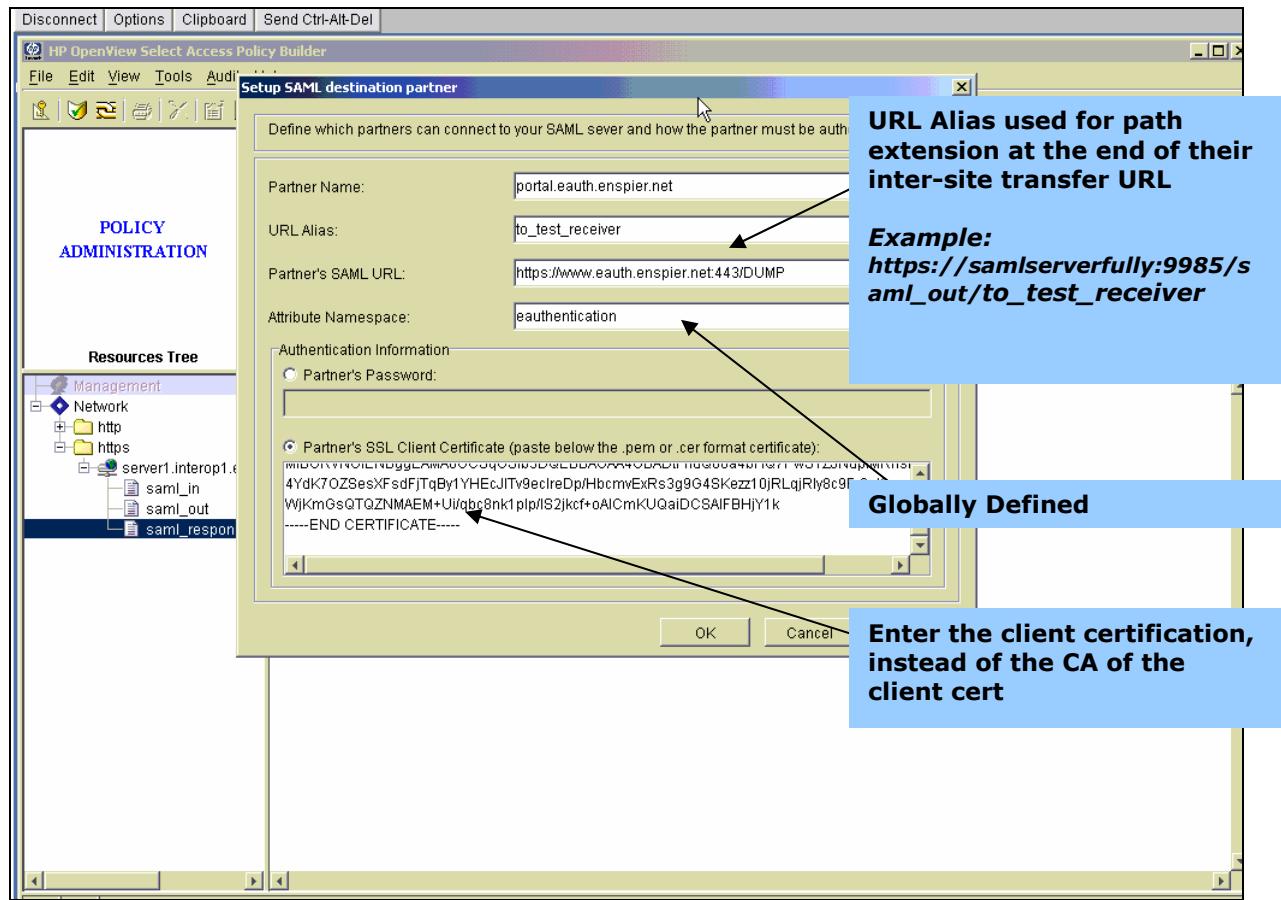


Figure 12-9: Configure AA Assertion Properties

2.3 Adding SAML Assertion Attribute

Right click on the *i* next to the SAML file you want to work with. Choose *SelectID Properties*.

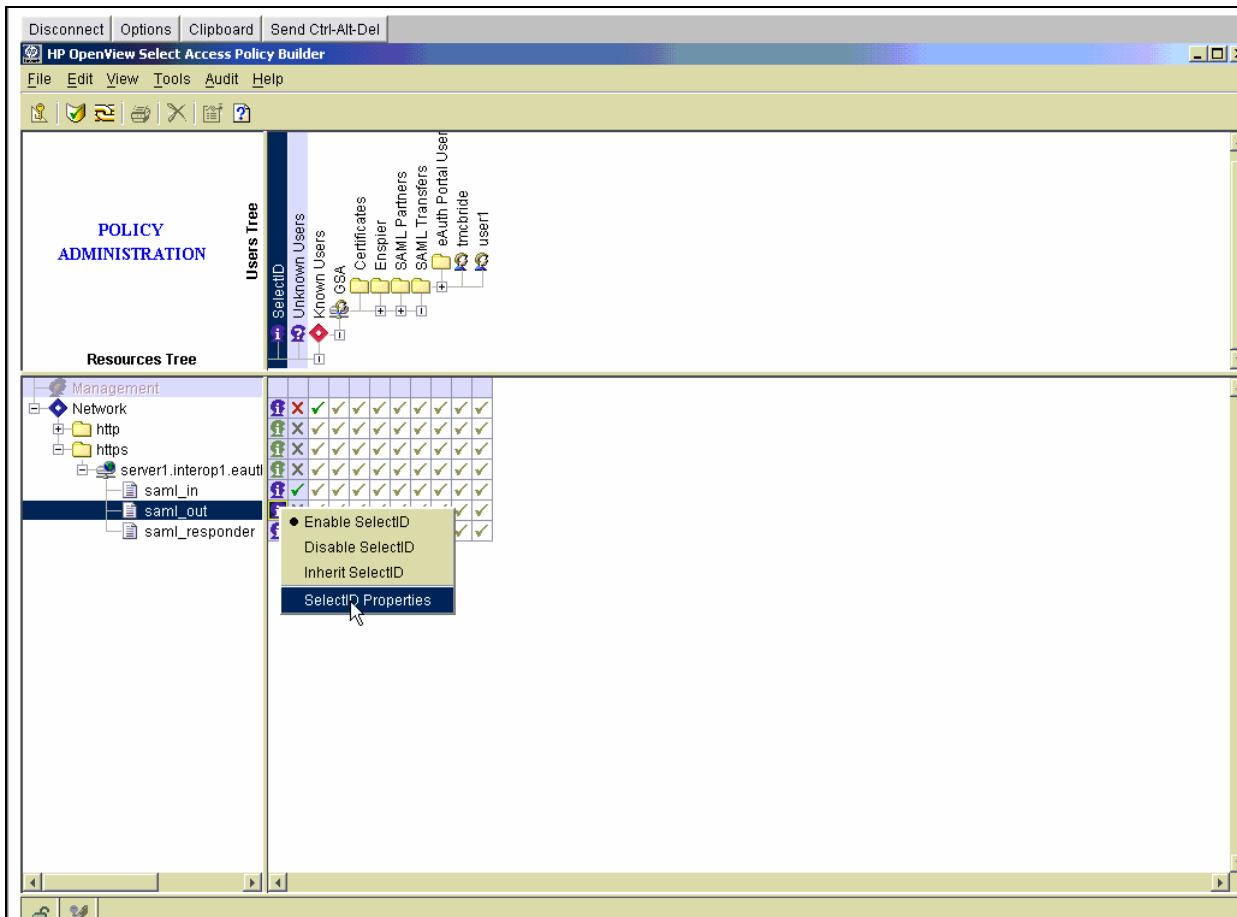


Figure 12-10: Configure AA Assertion Properties

The window shown in figure 12-11 will display, click on the *Personalization* tab when the window finishes loading.

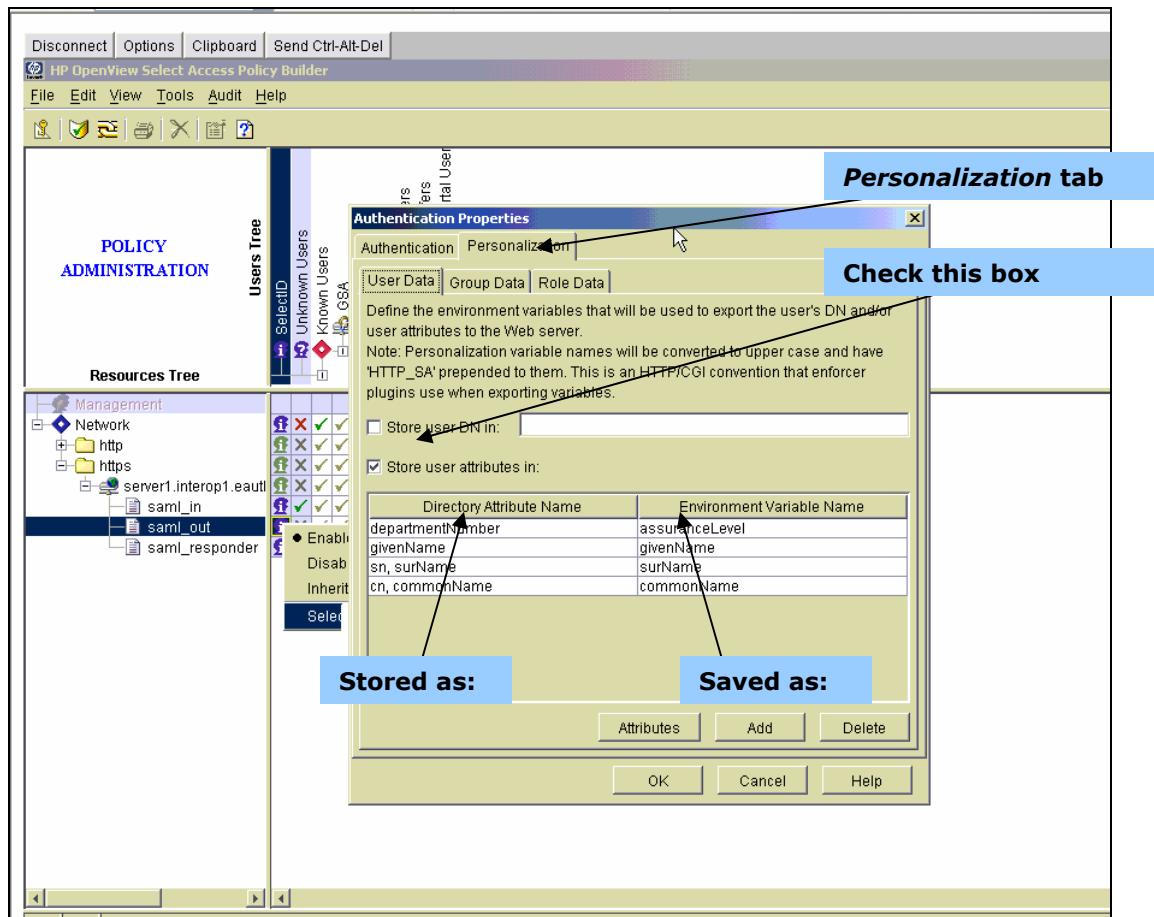


Figure 12-11: Personalization tab